

T S1/5/1

1/5/1

DIALOG(R)File 347:JAPIO

(c) 2004 JPO & JAPIO. All rts. reserv.

05499941 **Image available**
PORTABLE INFORMATION RECORDING MEDIUM

PUB. NO.: 09-114741 [JP 9114741 A]
PUBLISHED: May 02, 1997 (19970502)
INVENTOR(s): IRISAWA KAZUYOSHI
APPLICANT(s): DAINIPPON PRINTING CO LTD [000289] (A Japanese Company or
 Corporation), JP (Japan)
APPL. NO.: 07-294749 [JP 95294749]
FILED: October 18, 1995 (19951018)
INTL CLASS: [6] G06F-012/14; G06F-012/00; G06K-017/00; G06K-019/073
JAPIO CLASS: 45.2 (INFORMATION PROCESSING -- Memory Units); 45.3
 (INFORMATION PROCESSING -- Input Output Units)

ABSTRACT

PROBLEM TO BE SOLVED: To make possible an access with excellent operability, securing sufficient security, for the file having the hierarchical structure for which the separate security setting for every purpose is performed, by performing a specified processing by providing a CPU executing the command imparted from the outside and the first and second memories accessed by this CPU.

SOLUTION: When a command 'SELECT #3 DF 1-2' designating a specified channel and selecting a specified file control area is imparted, unlocking information is maintained as it is for recording parts (1, 3) for which discrimination information is not updated. When other recording parts (2, 2) in which the same discrimination information DF 1 as this updated discrimination is recorded exist for the recording part for which discrimination information is not updated, the unlocking information recorded in these other recording parts is copied as it is. When these other recording parts do not exist, a processing writing the unlocking information showing locking is performed.

?

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-114741

(43) 公開日 平成9年(1997)5月2日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 1 0		G 0 6 F 12/14	3 1 0 K
	5 3 7		12/00	5 3 7 A
G 0 6 K 17/00			G 0 6 K 17/00	E
19/073			19/00	P

審査請求 未請求 請求項の数 5 F D (全 18 頁)

(21) 出願番号 特願平7-294749

(22) 出願日 平成7年(1995)10月18日

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 入澤 和義

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(74) 代理人 弁理士 志村 浩

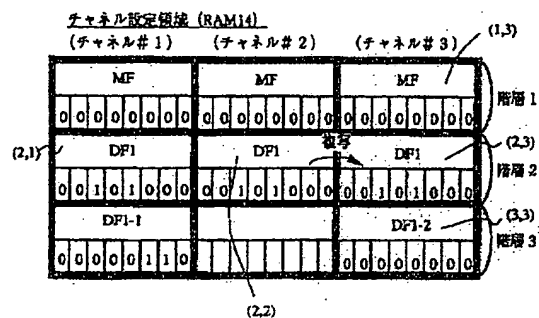
(54) 【発明の名称】 携帯可能情報記録媒体

(57) 【要約】

【課題】 用途ごとに別々のセキュリティ設定がなされ、階層構造をもったファイルに対し、十分なセキュリティを確保しつつ使い勝手の良いアクセスを行う。

【解決手段】 RAM内に、各チャンネルごとの開錠状態を示す記録部を各階層ごとに設ける。各チャンネル内には、そのチャンネルを用いて選択されたファイル管理領域DFへの階層上のパスが記録される。新たにチャンネル#3を用いてDF1-2を選択すると、MF→DF1→DF1-2なるパスが記録されるが、チャンネル#2にも存在するDF1の開錠状態は、チャンネル#3に複写される。いずれかのチャンネルにおいてDF1の開錠状態を更新すると、更新された開錠状態が他チャンネルのDF1へ複写される。必要に応じて上位階層の開錠状態を参照する旨の設定を行うと、上下両階層の開錠状態のビット間論理和により開錠状態が判断される。

① SELECT #3 DF1-2



【特許請求の範囲】

【請求項1】 外部から与えられるコマンドを実行するCPUと、このCPUによってアクセスされる第1のメモリと第2のメモリと、を備え、前記第1のメモリには、階層構造をもったファイル管理領域を定義して各ファイル管理領域内にそれぞれ所定のファイルを所定のアクセス条件とともに記録し、前記第2のメモリには、前記アクセス条件に関連した開錠情報を記録し、この開錠情報と各ファイルについてのアクセス条件とを比較することにより、前記第1のメモリ内の各ファイルに対するアクセスの可否を判定するようにした携帯可能情報記録媒体において、

前記第2のメモリ内に、複数のチャネル設定領域を設け、各チャネル設定領域を互いに上下の階層関係をもった複数の記録部に分割し、個々の記録部には、特定のファイル管理領域を示す識別情報と、この特定のファイル管理領域についての開錠情報と、を記録できるようにし、

特定のチャネルを指定して特定のファイル管理領域を選択するコマンドが与えられたときには、選択されたファイル管理領域およびこれより上位階層のファイル管理領域の識別情報を、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込んで記録済状態とし、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態とする書込処理を行い、この書込処理によって、識別情報が更新されなかった記録部については開錠情報をそのまま維持し、識別情報が更新された記録部については、この更新された識別情報と同一の識別情報が記録されている他の記録部が存在する場合には、前記他の記録部に記録されている開錠情報をそのまま複写し、そのような他の記録部が存在しない場合には、未開錠を示す開錠情報を書き込む処理を行い、特定のチャネルを指定して所定のキー照合を行うコマンドが与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている開錠情報をキー照合の結果に基づいて更新する更新処理を行い、前記最下層の記録部に記録されている識別情報と同一の識別情報が記録されている別な記録部が存在する場合には、前記更新処理によって更新された開錠情報を、前記別な記録部にそのまま複写する処理を行い、特定のチャネルを指定して所定の対象ファイルをアクセスするコマンドが与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている識別情報で特定されるファイル管理領域内に前記対象ファイルが所属し、かつ、前記最下層の記録部に記録されている開錠情報が、前記対象ファイルのアクセス条件を満足する場合に、前記対象ファイルに対するアクセスを可能とすることを特徴とする携帯可能情報記録媒体。

【請求項2】 請求項1に記載の携帯可能情報記録媒体

において、

各ファイル管理領域について、上位階層のファイル管理領域の開錠情報を参照するか否かの設定を行えるようにし、参照する旨の設定がなされていたときには、上位階層のファイル管理領域の開錠情報と自己の開錠情報とを融合させた融合開錠情報が、対象ファイルのアクセス条件を満足する場合に、前記対象ファイルに対するアクセスを可能とするようにしたことを特徴とする携帯可能情報記録媒体。

【請求項3】 請求項2に記載の携帯可能情報記録媒体において、

第2階層以下の各ファイル管理領域について、最上位階層のファイル管理領域の開錠情報を常に参照する旨の設定が行われていることを特徴とする携帯可能情報記録媒体。

【請求項4】 請求項1～3のいずれかに記載の携帯可能情報記録媒体において、

ファイルに対するアクセスコマンドを、そのアクセスの態様に応じて複数のグループに分け、各ファイルについてのアクセス条件を、各グループごとに設定するようにし、

アクセスコマンドが与えられたときには、このアクセスコマンドが所属するグループについて設定されているアクセス条件を開錠情報と比較するようにしたことを特徴とする携帯可能情報記録媒体。

【請求項5】 請求項1～4のいずれかに記載の携帯可能情報記録媒体において、

最上位階層については、複数のチャネルを代表する単一の記録部のみを設けるようにしたことを特徴とする携帯可能情報記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は携帯可能情報記録媒体、特に、CPUと、このCPUによってアクセスされるメモリとを備えた記録媒体に関する。

【0002】

【従来の技術】ICカードに代表される携帯可能情報記録媒体は、磁気カードに代わる次世代の媒体として注目を集めており、最近では、半導体集積回路の小型化、低コスト化のための技術革新により、実社会の種々のシステムにおいてICカードが実用されるに至っている。

【0003】特に、CPUを内蔵したICカードは、単なる情報記録媒体としての機能だけではなく、情報処理機能を有するため、高度なセキュリティを必要とする情報処理システムへの利用が期待されている。一般に、ICカードには、EEPROMなどの不揮発性メモリが内蔵されており、このEEPROM内にファイルとして情報が記録されることになる。しかも、EEPROMへのアクセスは、内蔵CPUによって行われるため、予め所定のアクセス条件を設定しておけば、内蔵CPUがこの

アクセス条件を満足したと判断したときのみ、ファイルへのアクセスを許可するようにすることができる。通常は、いくつかのキーについての照合をアクセス条件として設定する。すなわち、EEPROM内に予めキーを書き込んでおき、この内部のキーと外部から与えられたキーとを内蔵CPUで比較照合し、両者が一致した場合に、当該キーが開錠されたものと判断するのである。

【0004】キーとしては、特定の対象者（たとえば、ICカードの所有者、発行者など）を認証するためのキーや、特定のハードウェア（たとえば、端末装置）を認証するためのキーなどが利用されている。通常は、これらのキーを複数用い、ファイルに対するアクセス条件として、複数のキーの開錠を条件として設定することが多い。すなわち、特定のファイルに対するアクセス条件として、特定のキーの組み合わせが要求されることになる。個々のファイルごとに異なったアクセス条件を設定するために、各ファイルごとにそれぞれディレクトリ領域を設け、このディレクトリ領域内に、開錠を必要とするキーを指定する情報を書き込んでおくのが一般的である。この場合、各ファイルに対するアクセスコマンドが外部から与えられると、内蔵CPUは、まず、そのアクセス対象ファイルについてのディレクトリ領域を参照し、照合を必要とするキーについての開錠作業が完了している場合に限り、アクセスコマンドの実行を行うことになる。

【0005】

【発明が解決しようとする課題】ICカードは、磁気カードに比べてデータの記憶容量が大きく、内蔵した不揮発性メモリ内に多数のファイルを記録しておくことができる。しかも、EEPROMなどの内蔵不揮発性メモリの容量は、半導体集積回路の製造技術の進歩により、今後も益々増加してゆくものと期待されている。このため、1枚のICカードを複数の用途に利用する利用形態が一般化するものと予想される。たとえば、銀行用カード、クレジットカード、交通機関用プリペイドカード、病院用カード、といった複数の用途に対して、1枚のICカードで対応することが可能になる。

【0006】このような複数の用途に対応するICカードでは、個々の用途ごとにそれぞれ別個のファイルを用意する必要が生じ、各ファイルに対するアクセス条件もそれぞれ別個独立して設定する必要がある。しかも、用途の異なる複数のファイルを交互にアクセスするような利用形態も、今後は益々増えてゆくものと予想される。たとえば、病院用カードとしての部分に書き込まれた医療費を、銀行用カードとしての部分に書き込まれた預金残高から振り替えることにより、医療費の支払いを行うような場合、病院用ファイルと銀行用ファイルとを交互にアクセスする必要が生じる。この場合、病院用ファイルに対するセキュリティと銀行用カードに対するセキュ

リティとは、別個に設定されているため、各ファイルを

アクセスするごとにそれぞれ開錠操作が必要になり、使い勝手が悪いという問題が生じる。
【0007】このような多用途に対応したICカードについての使い勝手を向上させる手法として、アクセスチャネルという概念を導入し、個々のアクセスチャネルごとに開錠操作を行う方法が提案されている。たとえば、特開平7-160547号公報には、各チャネルごとにそれぞれ異なる識別番号を定義し、それぞれのチャネルごとに開錠状態を記録しておく方法が開示されている。しかしながら、階層構造をもったファイルについて、用途ごとに別々のセキュリティが設定されている場合に、種々のファイルを交錯してアクセスするには、十分な使い勝手が得られていないのが現状である。

【0008】そこで本発明は、用途ごとに別々のセキュリティ設定がなされ、しかも階層構造をもったファイルに対して、十分なセキュリティを確保しつつ使い勝手の良いアクセスが可能な携帯可能情報記録媒体を提供することを目的とする。

【0009】

【課題を解決するための手段】

(1) 本発明の第1の態様は、外部から与えられるコマンドを実行するCPUと、このCPUによってアクセスされる第1のメモリと第2のメモリと、を備え、第1のメモリには、階層構造をもったファイル管理領域を定義して各ファイル管理領域内にそれぞれ所定のファイルを所定のアクセス条件とともに記録し、第2のメモリには、アクセス条件に関連した開錠情報を記録し、この開錠情報と各ファイルについてのアクセス条件とを比較することにより、第1のメモリ内の各ファイルに対するアクセスの可否を判定するようにした携帯可能情報記録媒体において、第2のメモリ内に、複数のチャネル設定領域を設け、各チャネル設定領域を互いに上下の階層関係をもった複数の記録部に分割し、個々の記録部には、特定のファイル管理領域を示す識別情報と、この特定のファイル管理領域についての開錠情報と、を記録できるようにし、特定のチャネルを指定して特定のファイル管理領域を選択するコマンドが与えられたときには、選択されたファイル管理領域およびこれより上位階層のファイル管理領域の識別情報を、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込んで記録済状態とし、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態とする書込処理を行い、この書込処理によって、識別情報が更新されなかった記録部については開錠情報をそのまま維持し、識別情報が更新された記録部については、この更新された識別情報と同一の識別情報が記録されている他の記録部が存在する場合には、他の記録部に記録されている開錠情報をそのまま複写し、そのような他の記録部が存在しない場合には、未開錠を示す開錠情報を書き込む処理を行い、特定のチャネルを指定して所定のキー照合を行うコマンド

が与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている開錠情報をキー照合の結果に基づいて更新する更新処理を行い、この最下層の記録部に記録されている識別情報と同一の識別情報が記録されている別な記録部が存在する場合には、更新処理によって更新された開錠情報を、この別な記録部にそのまま複写する処理を行い、特定のチャネルを指定して所定の対象ファイルをアクセスするコマンドが与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている識別情報で特定されるファイル管理領域内に対象ファイルが所属し、かつ、この最下層の記録部に記録されている開錠情報が、対象ファイルのアクセス条件を満足する場合に、この対象ファイルに対するアクセスを可能とするようにしたものである。

【0010】(2) 本発明の第2の態様は、上述の第1の態様に係る携帯可能情報記録媒体において、各ファイル管理領域について、上位階層のファイル管理領域の開錠情報を参照する可否かの設定を行えるようにし、参照する旨の設定がなされていたときには、上位階層のファイル管理領域の開錠情報と自己の開錠情報とを融合させた融合開錠情報が、対象ファイルのアクセス条件を満足する場合に、対象ファイルに対するアクセスを可能とするようにしたものである。

【0011】(3) 本発明の第3の態様は、上述の第2の態様に係る携帯可能情報記録媒体において、第2階層以下の各ファイル管理領域について、最上位階層のファイル管理領域の開錠情報を常に参照する旨の設定を行うようにしたものである。

【0012】(4) 本発明の第4の態様は、上述の第1～第3に記載の携帯可能情報記録媒体において、ファイルに対するアクセスコマンドを、そのアクセスの態様に応じて複数のグループに分け、各ファイルについてのアクセス条件を、各グループごとに設定するようにし、アクセスコマンドが与えられたときには、このアクセスコマンドが所属するグループについて設定されているアクセス条件を開錠情報と比較するようにしたものである。

【0013】(5) 本発明の第5の態様は、上述の第1～第4に記載の携帯可能情報記録媒体において、最上位階層については、複数のチャネルを代表する単一の記録部のみを設けるようにしたものである。

【0014】

【発明の実施の形態】本発明に係る携帯可能情報記録媒体は、外部から与えられるコマンドを実行するCPUと、このCPUによってアクセスされる2種類のメモリとを有する。もっとも、この2種類のメモリは、その記録内容によって概念上区別されるだけのものであり、物理的には単一のメモリ素子を領域分割して用いてもかまわない。これら2種類のメモリのうち、第1のメモリには、この媒体に本来記録すべきファイルが、それぞれ所

定のアクセス条件とともに記録される。このアクセス条件は、そのファイルに対するアクセスを行うためには、どのキーを照合する必要があるかを示す条件である。一方、第2のメモリには、このアクセス条件に関連した開錠情報が記録される。具体的には、どのキーの照合が既に完了して開錠状態になっているか、という情報が記録されることになる。したがって、特定のファイルに対する読出コマンドや書込コマンドなどのアクセスコマンドが与えられた場合には、このアクセス対象となったファイルについてのアクセス条件と、その時点における開錠情報とを比較することにより、アクセスの可否が判定される。

【0015】本発明では、第1のメモリ内に、階層構造をもったファイル管理領域が定義される。このファイル管理領域は、概念的には、いわば具体的なファイルを入れる箱に相当するものであり、この箱を入れ子状にすることにより階層構造を採ることができる。具体的なファイルは、いずれかの箱の中に入れられることになる。セキュリティは、個々の箱ごとに別個に設定することができる。したがって、各用途ごとに別個の箱を用意しておけば、用途ごとに異なるセキュリティ設定が可能になる。

【0016】第2のメモリ内に記録される開錠情報も、個々の箱ごとに、すなわち、個々のファイル管理領域ごとに別個に記録される。しかも、実際のアクセスは「チャネル」という概念を用いて行われる。すなわち、まず特定のチャネルを指定して、特定のファイル管理領域（箱）を選択する。特定のチャネルについて、どの箱が選択されたかを示すために、第2のメモリ内には、複数のチャネル設定領域が設けられる。各チャネル設定領域は、上下の階層関係をもった複数の記録部に分割され、個々の記録部には、特定のファイル管理領域を示す識別情報と、この特定のファイル管理領域についての開錠情報と、が記録される。特定のチャネルを指定して特定のファイル管理領域（箱）を選択すると、この選択されたファイル管理領域（選択された箱）およびこれより上位階層のファイル管理領域（外側の箱）を示す識別情報が、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込まれる。このような書き込みが行われた記録部は記録済状態になる。このとき、選択されたファイル管理領域（選択された箱）より下位階層のファイル管理領域（内側の箱）に相当する記録部は未記録状態である。したがって、チャネル設定領域内の記録済の最下層の記録部が、常に、そのチャネルについて選択されたファイル管理領域（選択された箱）に対応することになる。

【0017】このように、チャネル設定領域には、選択されたファイル管理領域（箱）に至るまでの階層構造上のパスが記録されることになる。各チャネルごとに、それぞれ任意のファイル管理領域を選択することができる

ので、異なるチャンネルについて、部分的にバスが共通するファイル管理領域が選択されると、異なる記録部に同一のファイル管理領域を示す識別情報が記録されることになる。

【0018】各記録部には、ファイル管理領域(箱)を特定するための識別情報とともに、そのファイル管理領域(箱)についての開錠情報が記録される。すなわち、1つの記録部を参照すれば、ある1つの箱についての現時点における開錠状態が認識できることになる。本発明の重要な特徴は、この開錠情報の更新方法にある。各記録部の開錠情報は、次の2とおりの場合に更新される。第1の場合は、特定のチャンネルを指定して、特定のファイル管理領域(箱)を選択するコマンドが与えられたときである。この場合は、識別情報が更新されなかった記録部については、開錠情報もそのまま更新されずに維持される。すなわち、既に何らかの開錠操作が行われていた箱については、その開錠情報がそのまま維持されることになり、再度の開錠操作を行う必要はない。一方、識別情報が更新された記録部については、この更新された識別情報と同一の識別情報が記録されている他の記録部が存在する場合には、他の記録部に記録されている開錠情報をそのまま複写する。すなわち、他のチャンネルにおいて、同一のファイル管理領域(箱)に対して既に何らかの開錠操作が行われていた場合には、その開錠情報がそのまま複写されるので、別なチャンネルで同じファイル管理領域(箱)をアクセスする場合でも、再度の開錠操作を行う必要はなくなる。そして、そのような他の記録部が存在しない場合には、未開錠を示す開錠情報が書き込まれる。すなわち、その選択されたファイル管理領域(箱)について、過去にいずれかのチャンネルにおいて開錠操作が行われたという記録が残っていない場合には、未開錠なる開錠情報が書き込まれ、アクセスには所定の開錠操作が要求されることになる。

【0019】各記録部の開錠情報が更新される第2の場合は、特定のチャンネルを指定して所定のキー照合を行うコマンドが与えられたときである。前述したように、各チャンネル設定領域内の記録済状態にある最下層の記録部は、常に、そのチャンネルについて選択されたファイル管理領域(選択された箱)を示している。別言すれば、チャンネルの指定は、最下層の記録部に記録されたファイル管理領域(箱)の指定と同等の意味をもつ。そこで、このようなキー照合コマンドが与えられたときには、そのチャンネルの最下層の記録部に記録されたファイル管理領域(箱)についての照合処理が実行され、キー照合が一致すれば、そのキーが開錠状態になったことを示す開錠情報がこの記録部に書き込まれることになる。このように、キー照合コマンドの実行により、この記録部内の開錠情報が更新されることになるが、本発明では、この記録部に記録されている識別情報と同一の識別情報が記録されている別な記録部が存在する場合には、更新処理に

よって更新された開錠情報を、この別な記録部にもそのまま複写する処理が行われる。すなわち、ある1つのチャンネルについて、ある1つのファイル管理領域(箱)の開錠状態に変更があった場合には、別なチャンネルに記録されている同一のファイル管理領域(箱)の開錠状態にも同一の変更が加えられることになる。別言すれば、1つのチャンネルにおける開錠操作が、別なチャンネルにおいても反映されることになり、同一のファイル管理領域(箱)についての開錠操作を、アクセスチャンネルが変わるごとに繰り返す必要がなくなる。

【0020】本発明では、個々のファイルに対するアクセスも、チャンネルを指定して行うことになる。このようなアクセスコマンドが与えられると、まず、指定されたチャンネル設定領域内の記録済状態にある最下層の記録部に記録されている識別情報で特定されるファイル管理領域(箱)にアクセスの対象となるファイルが所属しているか否かが調べられる。指定されたチャンネルによって選択されているファイル管理領域(箱)に、アクセス対象ファイルが所属していなければ、チャンネル管轄外のファイルアクセスが行われたことになるので、アクセスは許可されない。アクセス対象ファイルが、チャンネルで選択されているファイル管理領域(箱)に所属している場合には、このファイル管理領域(箱)についての開錠情報が、対象ファイルのアクセス条件を満足しているか否かが調べられ、満足している場合には、この対象ファイルに対するアクセスが行われることになる。

【0021】

【実施例】

§1. ICカードの基本構成

以下、本発明を図示する実施例に基づいて説明する。図1は、一般的なICカード10に、外部装置としてのリーダライタ装置20を接続し、アクセスを行っている状態を示すブロック図である。ICカード10とリーダライタ装置20とはI/Oライン30によって相互に接続されている。ここで、ICカード10には、I/Oインタフェース11、CPU12、ROM13、RAM14、EEPROM15が内蔵されている。I/Oインタフェース11は、I/Oライン30を介してデータを送受するための入出力回路であり、CPU12はこのI/Oインタフェース11を介して、リーダライタ装置20と通信することになる。ROM13内には、CPU12によって実行されるべきプログラムが記憶されており、CPU12はこのプログラムに基づいて、ICカード10を統括制御する機能を有する。RAM14は、CPU12がこのような統括制御を行う上での作業領域として使用されるメモリである。一方、EEPROM15は、このICカード10に記録すべき本来のデータを格納するメモリである。

【0022】このICカード10に対しては、外部のリーダライタ装置20から電源やクロックが供給される。

したがって、ICカード10がリーダライタ装置20と切り離されると、ICカード10への電源およびクロックの供給は停止する。しかしながら、EEPROM15は不揮発性メモリであるため、電源供給が停止した後もその記録内容はそのまま保持される。ただ、RAM14内のデータは、電源供給の停止によりすべて失われる。

【0023】ICカード10内の各メモリ13、14、15へのアクセスは、すべてCPU12を介して行われ、外部からこれらメモリを直接アクセスすることはできない。すなわち、リーダライタ装置20からCPU12に対して所定の「コマンド」を与えると、CPU12はこの「コマンド」を解釈実行し、その結果を、リーダライタ装置20に対して「レスポンス」として返送することになる。たとえば、EEPROM15内の所定のファイルに書き込みを行う場合には、「書込コマンド」とともに書込対象となるデータをCPU12に与え、CPU12による「書込コマンド」の実行という形式で書込処理が行われることになる。逆に、EEPROM15内の所定のファイルからデータの読出しを行う場合は、所定の「読出コマンド」をCPU12に与え、CPU12

による「読出コマンド」の実行という形式で読出処理が行われることになる。このように、ICカード10内において「コマンド」の実行が終了すると、実行した「コマンド」に対する「レスポンス」が外部に対して返送される。たとえば、「書込コマンド」を与えた場合には、書込処理が支障なく実行されたか否かを示す「レスポンス」が返送され、「読出コマンド」を与えた場合には、読出対象となったデータがレスポンスという形で返送されることになる。

【0024】ただし、上述のようなEEPROM15への

アクセスは、無条件で行われるわけではなく、所定のアクセス条件が満足されることが前提となる。このアクセス条件は、個々のファイルごとに、また、個々のコマンドグループごとに設定される。これについては後述する。

【0025】EEPROM15内には、階層構造をもったファイル管理領域が定義される。既に述べたように、このファイル管理領域は、概念的には、いわば具体的なファイルを入れる箱に相当するものであり、一般的には、このファイル管理領域は「Dedicated File」と呼ばれている。そこで本実施例では、このファイル管理領域を「DF」なる記号で示すことにし、特に、最上階層のファイル管理領域を「Master File」の意味を示す記号「MF」で表すことにする。図2は、階層構造をもった具体的なファイル管理領域を、EEPROM15内に定義した状態を示す概念図である。最上階層に相当する階層1には、ファイル管理領域MFが定義され、その中に、階層2に相当するファイル管理領域DF1、DF2が定義され、それぞれの中に、階層3に相当するファイル管理領域DF1-1、DF1-2、DF2-1、DF

2-2が定義されている。各ファイル管理領域内に示されている円で囲ったDおよびKは、それぞれ具体的なデータファイルおよびキーファイルを示す。各ファイル管理領域が「箱」であるのに対し、データファイルDおよびキーファイルKは、具体的な情報をもったファイルである。データファイルDは、本来記録すべきデータを収容したファイルであり、キーファイルKは、セキュリティ管理のために用いられるキー暗証コードを収容したファイルである。

【0026】図3は、図2に示すファイル管理領域および各ファイルの階層構造を示すツリー図である。四角で囲ったブロックはいずれもファイル管理領域（箱）を示し、楕円で囲ったブロックは個々のデータファイル（頭に記号Dのついたファイル）およびキーファイル（頭に記号Kのついたファイル）を示す。説明の便宜上、この図3では、個々のデータファイルおよびキーファイルを特定するために、K11、D112などの番号を付して示してある。たとえば、ファイルK00、K01、D00、D01は、階層1のファイル管理領域MFの管理下にあるファイルであり、ファイルK11、K12、D11、D12は、階層2のファイル管理領域DF1の管理下にあるファイルであり、ファイルK111、K112、D111、D112は、階層3のファイル管理領域DF1-1の管理下にあるファイルである。

【0027】このように、階層をもったファイル管理領域を定義すると、各ファイルを用途ごとに分けて管理することができる。この実施例では、このICカード10を、銀行用カード兼病院用カードとして利用する場合を述べる。図4は、各ファイル管理領域に、それぞれ大まかな用途を定義した一例を示すブロック図である。階層1のファイル管理領域MFは、このICカード10全体を統括管理する領域であり、その管理下にあるデータファイルD00、D01には、たとえば、このICカード10の所有者の氏名、住所、電話番号などの情報が記録される。これに対し、階層2のファイル管理領域DF1は、銀行業務を統括管理する領域であり、その管理下にあるデータファイルD11、D12には、たとえば、銀行がこのICカード10の所有者に付与した顧客番号、担保明細、信用情報などが記録される。また、同じ階層2のファイル管理領域DF2は、病院業務を統括管理する領域であり、その管理下にあるデータファイルD21、D22には、たとえば、病院がこのICカード10の所有者に付与した患者番号、血液型、身長、体重、緊急連絡先などの情報が記録される。

【0028】階層3のファイル管理領域DF1-1、DF1-2、DF2-1、DF2-2は、階層2の業務を更に細分化した個別の業務を管理する領域である。たとえば、ファイル管理領域DF1-1は、銀行業務のうちの国内預金を管理する領域であり、その管理下にあるデータファイルD111、D112には、たとえば、普通

預金あるいは定期預金の口座取引情報が記録される。また、ファイル管理領域DF1-2は、銀行業務のうちの外国為替を管理する領域であり、その管理下にあるデータファイルD121、D122には、たとえば、ドル立預金の取引情報や外国送金情報などが記録される。一方、ファイル管理領域DF2-1は、病院業務のうちの診療データを管理する領域であり、その管理下にあるデータファイルD211、D212には、たとえば、血液検査、レントゲン検査などの検査情報や、投薬情報などが記録される。また、ファイル管理領域DF2-2は、病院業務のうちの医療費データを管理する領域であり、その管理下にあるデータファイルD221、D222には、たとえば、初診料、診察料、健康保険点数などの情報が記録される。

【0029】§2. セキュリティの設定方法

さて、図3に示す階層構造では、階層1に4個のファイル、階層2に8個のファイル、階層3に16個のファイル、がそれぞれ定義されているが、これら各ファイルには、それぞれ独立したアクセス条件が設定されている。図5は、1つのファイルについてのアクセス条件の設定例を示すアクセス条件テーブルである。この実施例では、アクセス条件は、コマンドグループごとに設定されている。すなわち、各ファイルに対するアクセスコマンドは、そのアクセスの態様に依りて複数のグループに分けられる。この実施例では、キー照合を行うコマンドの集合であるコマンドグループ0と、情報の読出しを行うコマンドの集合であるコマンドグループ1と、情報の追記を行うコマンドの集合であるコマンドグループ2と、情報の書換え/消去を行うコマンドの集合であるコマンドグループ3と、の4つのグループが定義されている。ただ、コマンドグループ0は、無条件でアクセス可能という設定がなされているため、アクセス条件は、コマンドグループ1~3の3つのコマンドグループについてのみ設定されている。

【0030】図5に示すアクセス条件は、各コマンドグループのコマンドを実行するために、開錠が必要とされるキーを特定するテーブルから構成されている。すなわち、このアクセス条件テーブルは、各コマンドグループごとに8ビットの情報からなり、各ビットは、キーK1~K8までの8種類のキーについて、それぞれ開錠が必要であるか否かを示している。具体的には、ビット“1”は開錠必要を示し、ビット“0”は開錠不要を示す。たとえば、図5に示すようなアクセス条件が設定されたファイルに対して、情報の読出しを行うコマンドを実行する場合には、コマンドグループ1においてビット“1”が設定されている2つのキーK3、K5についての開錠が行われていなければならない。

【0031】図5に示すアクセス条件テーブルには、更に、Rと記された9番目のビットが設けられているが、この9番目のビットは、上位階層の開錠情報の参照の有

無を示す参照ビットである。すなわち、この参照ビットRに“1”が設定されていると、上位階層の開錠情報を参照することを意味し、“0”が設定されていると、上位階層の開錠情報を参照しないことを意味する。この参照ビットRの取り扱いについては、後に詳述する。

【0032】既に述べたように、図5に示すようなアクセス条件テーブルは、図3に楕円で示したすべてのファイル（データファイルおよびキーファイル）について、それぞれ設定されており、これらの各ファイルは、このアクセス条件テーブルとともに、EEPROM15に書き込まれていることになる。より具体的には、各ファイルには、それぞれ対応するディレクトリ領域が設けられ、このディレクトリ領域内に、各ファイルの先頭アドレスやファイル長が記録されるとともに、アクセス条件テーブルが記録されることになる。

【0033】一方、RAM14内には、開錠情報が記録される。この開錠情報は、図5に示すアクセス条件テーブルの各キーについて、開錠されたか否かを示すものであり、たとえば、図6(a)に示すような8ビットの領域がRAM14内に確保される。この8ビットの領域は、それぞれキーK1~K8の開錠状態を示しており、ビット“1”は開錠、ビット“0”は未開錠を示す。既に述べたように、ICカード10をリーダライタ装置20に接続すると、電源やクロックの供給が行われ、RAM14の記録内容はリセット状態となる。図6(a)に示す8ビットの開錠情報は、このリセット時において「00000000」の状態、すなわち、キーK1~K8のいずれもが未開錠の状態となる。たとえば、キー照合コマンド「VERIFY K3 ????」をリーダライタ装置20からICカード10に与えると(????の部分には、具体的なキー暗証コードがくる)、CPU12は、所定のキーファイルからキーK3に対応するキー暗証コードを読出し、これを外部から与えられたキー暗証コード「????」と比較照合し、両者が一致していれば、図6(b)に示すように、RAM14内の開錠情報の第3ビットK3にビット“1”を書き込み、キーK3が開錠状態になったことを示す。続いて、キー照合コマンド「VERIFY K5 ????」を与えて照合を行えば、図6(c)に示すように、RAM14内の開錠情報の第5ビットK5にもビット“1”が書き込まれる。こうして、2つのキーK3、K5が開錠状態になれば、図5に示すようなアクセス条件が設定されているファイルに対して、コマンドグループ1に属するコマンドの実行が可能になる。

【0034】以上、RAM14内の開錠情報に基づくアクセス可否判定の基本原理解を述べたが、本発明の特徴のひとつは、このRAM14内の開錠情報を、チャネルごとに、階層ごとに記録する点にある。すなわち、本発明では、RAM14内の開錠情報は、図6に示すような単純な構成で記録されるのではなく、図7に示すような構成

をもったチャネル設定領域をRAM14内に設定し、このチャネル設定領域内に記録されることになる。この図7に示す例では、3つのチャネル設定領域（チャネル#1、#2、#3）が定義されており、各チャネル設定領域は、互いに上下の階層関係をもった3つの記録部に分割されている。すなわち、3つのチャネル設定領域のそれぞれが、階層1～3の3つの記録部に分割され、合計9個の記録部が形成されている。ここで各記録部には、特定のファイル管理領域を示す識別情報を記録する領域（上段）と、この特定のファイル管理領域についての開錠情報を記録する領域（8区画に分割された下段）と、が設けられている。この下段の記録領域には、図6に示したような8ビットからなる開錠情報が記録され、この開錠情報と、図5に示したアクセス条件テーブルとを比較して、アクセスの可否判定が行われることになる。

【0035】§3. 具体的な利用態様を示す実施例

続いて、上述したICカードの具体的な利用態様を、図7に示すチャネル設定領域の記録内容の変遷を追いながら説明する。この実施例では、ICカード10をリーダライタ装置20に接続した直後のリセット時には、RAM14内のチャネル設定領域の記録内容は、図8に示すような初期状態になる。すなわち、各記録部上段には、識別情報が未記録であることを示す「FFFF」なる2バイトのデータが書き込まれ、各記録部下段には、8個のキーすべてが未開錠であることを示す「00000000」なる1ビットのデータが書き込まれる。なお、以下の説明では、便宜上、この9個の記録部を図8に示すように、記録部（1，1）、記録部（1，2）、…、記録部（3，3）と呼ぶことにする。

【0036】<3-1: ファイル管理領域の選択その1>本発明では、各ファイルをアクセスする準備段階として、特定のチャネルを指定して特定のファイル管理領域を選択する作業が必要になる。この作業を行うためには、リーダライタ装置20からICカード10に対して、所定のフォーマットをもった選択コマンドを与えればよい。ここでは、たとえば、図9①に示すように、「SELECT #1 DF1」なるフォーマットで、選択コマンドを与えた場合を考える。この選択コマンドは、特定のチャネル#1を指定して、特定のファイル管理領域DF1を選択するコマンドである。このようなコマンドが与えられると、CPU12は、選択されたファイル管理領域DF1およびこれより上位階層のファイル管理領域MFの識別情報を、指定されたチャネル設定領域（チャネル#1）内のそれぞれの階層に対応した記録部の上段に書き込んで記録済状態とし、各記録部下段にはすべてのキーが未開錠であることを示す開錠情報を書き込む処理を行う。図9は、このような処理が行われた直後のチャネル設定領域の状態を示している。各記録部の上段には、実際には、特定のファイル管理領域を示す2バイトの識別情報が書き込まれるが、図では、説明

の便宜上、各ファイル管理領域名（MF、DF1）を直接書き込んだ状態を示してある。また、図が複雑になるのを避けるため、説明に直接関連しない未記録状態の記録部は空欄にして示すことにするが、実際には、これらの空欄には、図8に示すように、「FFFF（上段）」もしくは「00000000（下段）」なるデータが書き込まれている。

【0037】結局、各チャネル設定領域を構成する記録部のうち、上段が「FFFF」である記録部は未記録状態の記録部を示し、上段が「FFFF」以外である記録部は記録済状態の記録部を示す。そして、各チャネル設定領域において、記録済状態にある最下層の記録部に識別情報が記録されているファイル管理領域が、当該チャネルについて現在選択されているファイル管理領域となる。図9に示す例の場合、チャネル#1の領域において、記録済状態にある最下層の記録部（2，1）には、ファイル管理領域DF1を示す識別情報が書き込まれているので、チャネル#1について現在選択されているファイル管理領域は、DF1ということになる。このとき、チャネル#1の上位階層の記録部（1，1）には、ファイル管理領域MFの識別情報が書き込まれているが、これは、現在選択されているファイル管理領域DF1の階層構造上の親がMFであることを示す役目を果たすとともに、後述するように、上位階層の開錠情報を参照する設定を可能にするためのものである。

【0038】本発明では、このように特定のチャネルを指定して特定のファイル管理領域を選択するコマンドが与えられたときには、選択されたファイル管理領域およびこれより上位階層のファイル管理領域の識別情報が、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込まれ、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態とされる。したがって、たとえば、図9①に示す「SELECT #1 DF1」なる選択コマンドの代わりに、図10①に示す「SELECT #1 DF1-2」なる選択コマンドを与えて、階層3のファイル管理領域DF1-2を選択した場合には、チャネル#1の記録内容は図10に示すようなものになる。この図10では、記録済状態にある最下層の記録部（3，1）には、ファイル管理領域DF1-2を示す識別情報が書き込まれているので、チャネル#1について現在選択されているファイル管理領域は、DF1-2ということになる。

【0039】<3-2: キーの照合その1>続いて、キーの照合が行われた場合の、チャネル設定領域の更新処理を説明する。本発明では、キーの照合は、特定のチャネルを指定して所定のキー照合を行うコマンドを与えることによって行われる。たとえば、いま、図9に示すように、チャネル#1としてファイル管理領域DF1が選択されている状態において、この選択されているファイル管理領域DF1についてのキー照合を行う場合を考え

る。ここでは、キーK3とキーK5の照合を行うものとしよう。この場合、まず、図11①に示すような「VERIFY #1 K3 ????」なる照合コマンドを与えればよい。ここで、「????」は具体的なキー暗証コードであり、CPU12は、チャンネル#1として選択されているファイル管理領域DF1内の所定のキーファイルから、キーK3の暗証コードを読み出し、これを外部から与えられたキー暗証コード「????」と比較照合する。そして、両者が一致すれば、図11の記録部(2, 1)の下段第3ビット目に開錠状態を示すビット

“1”を書き込む処理を行う。続いて、図11②に示すような「VERIFY #1 K5 ????」なる照合コマンドが与えられたら、キーK5の照合を行い、一致すれば、第5ビット目にビット“1”を書き込む処理を行う。図11に示す記録部(2, 1)のビット状態は、このような処理が行われた直後の状態を示している。

【0040】結局、本発明において、特定のチャンネルを指定して所定のキー照合を行うコマンドが与えられた場合には、指定されたチャンネル設定領域内の記録済状態にある最下層の記録部(上述の例の場合、記録部(2, 1))に記録されている開錠情報を、キー照合の結果に

基いて更新する更新処理が行われることになる。

【0041】<3-3: ファイルのアクセス>本発明におけるファイルのアクセスは、特定のチャンネルを指定して所定の対象ファイルをアクセスするコマンドを与えることによって行われる。たとえば、図4に示すような用途が定義されている状態において、銀行業務全般に用いるデータ(たとえば、顧客番号)を、ファイル管理領域DF1の管理下にあるデータファイルD11から読み出す処理を行う場合を考えよう。ここでは、より具体的

に、データファイルD11内の第8レコードを読み出すことにする。本発明では、このように特定のファイルをアクセスする場合も、必ず特定のチャンネルを指定する必要がある。しかも、指定するチャンネルは、アクセス対象ファイルを管理するファイル管理領域を現在選択中のチャンネルでなければならない。別言すれば、特定のファイルをアクセスするコマンドを与える前には、必ず、そのアクセス対象ファイルを管理するファイル管理領域を特定のチャンネルを用いて選択しておく必要がある。

【0042】上述の実施例の場合、図9①に示す「SELECT #1 DF1」なる選択コマンドにより、チャンネル#1を用いてファイル管理領域DF1を選択し、更に、図11①、②に示す照合コマンドにより、キーK3、K5を開錠状態にしておけば、データファイルD11内の第8レコードを読み出すことが可能になる。具体的には、図11③に示す「READ #1 D11 REC8」なるアクセスコマンドを与えればよい。CPU12は、このようなファイルアクセスのコマンドを受け取ると、まず、指定されたチャンネル設定領域内の記録済状態にある最下層の記録部(この例の場合、記録部

(2, 1))に記録されている識別情報で特定されるファイル管理領域(この例の場合、ファイル管理領域DF1)内に、アクセスの対象ファイル(この例の場合、データファイルD11)が所属しているか否かを判断する。もし所属していなかった場合には、アクセス対象ファイルが発見できない旨のエラーレスポンスがリーダー装置20側に伝達される。上述の例の場合、アクセスの対象ファイルD11は、ファイル管理領域DF1内に所属しているファイルとして発見されるので、エラーは生じない。

【0043】アクセス対象のファイルが発見されたら、続いて、アクセス条件が満たされているか否かの判定が行われる。すなわち、CPU12は、指定されたチャンネル設定領域内の記録済状態にある最下層の記録部(この例の場合、記録部(2, 1))に記録されている開錠情報(この例の場合、「00101000」と、アクセス対象のファイルについて設定されているアクセス条件(たとえば、図5に示すようなアクセス条件テーブル)と、を比較し、アクセス条件が満たされているか否かを判断するのである。この例の場合、「READ」なるコマンドは、コマンドグループ1に所属する読み出しコマンドであるから、図5のアクセス条件テーブルによれば、キーK3およびK5が開錠状態になっていれば、アクセス可能である。図11に示す記録部(2, 1)の開錠情報は、この条件を満たしている。よって、データファイルD11に対するアクセスは許可され、第8レコードの内容がリーダー装置20側へ読み出されることになる。

【0044】<3-4: ファイル管理領域の選択その2>図11に示す状態では、チャンネル#1を用いてファイル管理領域DF1が選択状態となっているので、チャンネル#1を指定したアクセスコマンドでは、ファイル管理領域DF1の管理下にあるファイルしかアクセスすることはできない。たとえば、ここで、外国為替に関する処理を行うために、ファイル管理領域DF1-2の管理下にあるデータファイルD121をアクセスする必要があるとしよう。この場合、新たに、ファイル管理領域DF1-2を選択しなおす必要がある。そこで、図12①に示すような選択コマンド「SELECT #1 DF1-2」を与えたとする。すると、チャンネル設定領域の状態は、図12に示すようになる。図12と図11との相違点は、図12では、新たに記録部(3, 1)が記録済状態になっている点である。ここで留意すべき点は、図11における記録部(2, 1)の開錠状態が、図12においてもそのまま維持されている点である。

【0045】この留意点は、図12と図10とを比較すればより明確になる。図10は、図8に示す初期状態において「SELECT #1 DF1-2」なる選択コマンドを与えた状態を示すのに対し、図12は、図11に示す中途状態において「SELECT #1 DF1

10

20

30

40

50

「2」なる同じ選択コマンドを与えた状態を示す。別言すれば、図10に示す状態は、何もない初期状態からファイル管理領域DF1-2に至るまでの階層上のパスを定義した場合に得られる状態であるのに対し、図12に示す状態は、図11に示すように、ファイル管理領域DF1に至るまでの階層上のパスを更に階層3のファイル管理領域DF1-2まで伸ばした場合に得られる状態であると言える。このようにパスを伸ばした場合には、伸ばした部分についての開錠状態は、未開錠を示す「00000000」が設定されるが、もとの部分についての開錠状態はもとの状態がそのまま維持されることになる。

【0046】要するに、所定のチャネルを用いてファイル管理領域を選択する選択コマンドが実行された場合、識別情報が更新されなかった記録部（図12の例の場合、記録部（1，1）および記録部（2，1））については開錠情報をそのまま維持し、識別情報が更新された記録部（図12の例の場合、記録部（3，1））については未開錠を示す開錠情報「00000000」を書き込む処理が実行されることになる。

【0047】<3-5：上位階層の開錠情報の参照>さて、図12に示す状態では、チャネル#1を用いてファイル管理領域DF1-2が選択されているので、このファイル管理領域DF1-2に対するキー照合処理を行い、必要な開錠操作を行えば、ファイル管理領域DF1-2の管理下にあるデータファイルD121に対するアクセスが許可されることになる。たとえば、データファイルD121からデータを読み出すためのアクセス条件として、3つのキーK3、K5、K6の開錠が要求されていたとしよう。この場合、図13①の「VERIFY #1 K3 ????」、図13②の「VERIFY #1 K5 ????」、図13③の「VERIFY #1 K6 ????」なるキー照合コマンドを与えて開錠操作を行えば、チャネル設定領域は図13に示すような状態となり、記録部（3，1）に、3つのキーK3、K5、K6が開錠状態となったことが記録される。そこで、更に、図13④の「READ #1 D121 REC5」なるアクセスコマンドを与えれば、アクセス条件は満足されているため、データファイルD121の第5レコードがリーダライタ装置20側に読み出されることになる。

【0048】しかしながら、図11①、②において、既にキーK3、K5の照合は完了しているので、図13①、②におけるキーK3、K5の照合処理は、冗長な処理操作となっている。実用上は、このように階層間で同一のキー照合をアクセス条件に設定することが少なくなる。たとえば、図4に示すように、銀行業務全般を管理するファイル管理領域DF1においては、銀行顧客認証キーK3と銀行支店認証キーK5との照合をアクセス条件として設定し、その下位階層のファイル管理領域DF

1-2においては、これらのキー照合に加えて、更に外国為替取扱権限キーK6の照合を付加的なアクセス条件として設定するというような利用形態は、実用上、多用される利用形態である。このような場合、ファイル管理領域DF1のアクセス時に既にキーK3、K5の照合が完了しているのであれば、続いてファイル管理領域DF1-2をアクセスする時には、キーK6の照合を行うだけで十分である。図5のアクセス条件テーブルにおいて示した参照ビットRは、このような便宜を考えて設けたものである。

【0049】たとえば、データファイルD121に対して読出しコマンドを実行するためのアクセス条件テーブルの参照ビットRが、ビット「1」（参照する）に設定されていた場合には、図13①～④の代わりに、図14①、②の2つのコマンドを与えるだけで、データファイルD121の第5レコードがリーダライタ装置20側に読み出されることになる。この場合、ファイル管理領域DF1-2を選択した状態でのキー照合は、キーK6についてのみ行われ、記録部（3，1）の開錠情報は、図14に示すように、キーK6のビットのみが「1」（開錠状態）となる。しかしながら、上位階層の開錠情報（この例の場合、記録部（2，1）の開錠情報）が参照されるので、ファイル管理領域DF1-2の開錠情報は、その上位階層のファイル管理領域DF1の開錠情報「00101000」と自己の開錠情報「000001000」とを融合させた融合開錠情報「001011000」（この実施例の場合、融合開錠情報は個々の開錠情報の各ビットごとの論理和をとることにより得られる）として取り扱われることになり、アクセス条件は満足されていると判断されることになる。

【0050】このように、上位階層の開錠情報を参照できる旨の設定を行っておけば、冗長な照合処理を省略することができ、十分なセキュリティを確保しつつ使い勝手の良いアクセスが可能になる。もちろん、高度なセキュリティを必要とするファイルに対しては、参照ビットRを「0」とし、参照を行わないような設定にしておけばよい。

【0051】<3-6：ファイル管理領域の選択その3>さて、外国為替に関するデータファイルD121のアクセスが完了した後に、銀行業務一般用のデータファイルD11を再度アクセスする必要がある場合を考えよう。この場合、データファイルD11を管理するファイル管理領域DF1を再度選択しなければならない。それには、図15①に示すように、「SELECT #1 DF1」なる選択コマンドを実行すればよい。これにより、チャネル設定領域は図15に示す状態に更新される。図14と図15とを比較すればわかるように、図15では、記録部（3，1）が初期状態（未記録状態）に戻されている。このように階層3を未記録状態にすれば、記録済状態にある最下層の記録部（2，1）には、

10

20

30

40

50

ファイル管理領域DF1の識別情報が書き込まれているので、現時点で、チャンネル#1はファイル管理領域DF1を選択している状態に戻ることになる。

【0052】このように、特定のファイル管理領域の選択を行った場合、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態となり、開錠情報は未開錠を示す「00000000」となる点は留意すべきである。このように、下位階層のファイル管理領域を選択していた状態から、その上位階層のファイル管理領域を選択する状態に移行した場合、下位階層の開錠情報を初期状態（未開錠状態）に戻すことは、セキュリティを確保する上で重要である。一般に、階層構造をもったファイル管理領域を構築した場合、下位階層へゆくに從って、より高度なセキュリティが要求される。したがって、上位階層へ戻った場合には、下位階層についての開錠情報を初期状態に戻し、再び下位階層へのアクセスを行う場合には、再度の開錠操作が要求されるようにしておくのが、セキュリティ確保の上からは好ましい。

【0053】<3-7:ファイル管理領域の選択その4>上述したように、選択ファイル管理領域を上位階層に戻した場合、下位階層の開錠情報は未開錠状態に戻される。すなわち、図14から図15への変遷により、記録部(3,1)の情報は失われることになる。このような処理は、セキュリティを確保する上では好ましいが、使い勝手の良いアクセスを行う上では障害となる。たとえば、データファイルD11とD121とを交互にアクセスする必要が生じた場合、ファイル管理領域DF1とDF2-1とを交互に選択しなければならないが、上位階層のファイル管理領域DF1を選択した時点で、図15に示すように、下位階層のファイル管理領域DF1-2の開錠情報が失われてしまうため、同じ照合操作を何度も繰り返さなくてはならなくなる。このような弊害を避けるためには、別なチャンネルを用いた選択を行えばよい。

【0054】たとえば、図14に示す状態において、図15①の「SELECT #1 DF1」なる選択コマンドを与える代わりに、図16①の「SELECT #2 DF1」なる選択コマンドを与えるのである。すると、図16に示すように、チャンネル#1を用いてファイル管理領域DF1-2を選択した状態のまま、チャンネル#2を用いてファイル管理領域DF1を選択することが可能になる。チャンネル#2の各記録部には、選択されたファイル管理領域DF1およびその上位階層のファイル管理領域MFの識別情報が書き込まれる。

【0055】ここで留意すべき点は、図16において、記録部(1,1)内の開錠情報が記録部(1,2)へ複写され、記録部(2,1)内の開錠情報が記録部(2,2)へ複写される点である。この複写処理の意図するところは、1つのチャンネルにおいて既に完了している照合処理については、別なチャンネルにおいても照合処理を不

要にすることである。図16に示す例では、チャンネル#1においてファイル管理領域DF1のキーK3、K5の照合処理が既に完了しているが、記録部(2,1)内の開錠情報が記録部(2,2)へ複写されるため、チャンネル#1においてもファイル管理領域DF1のキーK3、K5の照合処理が既に完了した状態となる。よって、チャンネル#2を用いてファイル管理領域DF1の管理下にあるファイルD11をアクセスする場合は、キーK3、K5の照合処理をあらためて行う必要はなく、図16②に示す「READ #2 D11 REC25」のようなアクセスコマンドを与えることにより、ファイルD11内の第25レコードの読出しが可能になる。

【0056】前述したように、特定のファイル管理領域を選択するコマンドが実行されると、チャンネル設定領域を構成する各記録部(この例の場合、記録部(1,2)および記録部(2,2))の識別情報が更新されることになるが、この更新された識別情報(この例の場合、MFおよびDF1)と同一の識別情報が記録されている他の記録部(この例の場合、記録部(1,1)および記録部(2,1))が存在する場合には、この他の記録部に記録されている開錠情報をそのまま複写する処理が行われることになる点が、本発明のひとつの特徴である。

【0057】<3-8:ファイル管理領域の選択その5>続いて、図16に示す状態において、今度は、医療費データに関するデータファイルD222をアクセスする必要が生じたため、図17①に示す「SELECT #1 DF2-2」なる選択コマンドを与えた場合を考える。この場合、チャンネル#1は図17のように更新されることになる。最上層のMFに変わりはないので、記録部(1,1)の記録内容は、開錠情報も含めてそのまま維持されるが、階層2、階層3は識別情報がDF2、DF2-2に更新され、それぞれの開錠情報は未開錠を示す状態になる。このように、チャンネル#1としては、記録部(2,1)の内容は、DF1からDF2へと更新されてしまうが、DF1の情報は記録部(2,2)に複写されているため、チャンネル#1が更新されたとしても、DF1の開錠情報はチャンネル#2としてそのまま残ることになる。ただし、図16において記録部(3,1)に記録されていたDF1-2の開錠情報は失われてしまう。

【0058】DF1-2の開錠情報をそのまま維持したい場合には、図17①に示す「SELECT #1 DF2-2」なる選択コマンドの代わりに、図18①に示す「SELECT #3 DF2-2」なる選択コマンドを与えればよい。すると、図18に示すように、チャンネル#1を用いてファイル管理領域DF1-2を選択し、チャンネル#2を用いてファイル管理領域DF1を選択した状態のまま、新たに、チャンネル#3を用いてファイル管理領域DF2-2を選択することが可能になる。チャンネル#3の各記録部には、選択されたファイル管理

領域DF 2-2およびその上位階層のファイル管理領域MF、DF 2の識別情報が書き込まれる。この場合もやはり、記録部(1, 2)内の開錠情報が記録部(1, 3)へと複写される。要するに、この複写処理は、同じ識別情報をもった記録部の開錠情報が常に同一となるようにするための処理と行うことができる。図18の例では、記録部(1, 1)、(1, 2)、(1, 3)は、いずれも同一の識別情報「MF」をもった記録部であるから、開錠情報は「00000000」と同一となり、記録部(2, 1)、(2, 2)は、いずれも同一の識別情報「DF 1」をもった記録部であるから、開錠情報は「00101000」と同一となっている。複写処理は、このような同一性を維持するための処理である。

【0059】さて、続いて、医療費データに関するデータファイルD222をアクセスするために、図19①に示す「VERIFY #3 K7 ????」なる照合コマンドおよび図19②に示す「VERIFY #3 K8 ????」なる照合コマンドを与えることにより、ファイル管理領域DF 2-2のキーK7、K8を開錠した場合を考える。この場合、図19に示すように、記録部(3, 3)には、キーK7、K8が開錠状態になったことが書き込まれる。そこで、図19③に示す「READ #3 D222 REC4」なる読出しコマンドを与えれば、データファイルD222の第4レコード(たとえば、医療費未精算額)がリーダー装置20側へと読み出されることになる。

【0060】ここで、この医療費未精算額について、国内預金データを示すファイルD111を書換えて振替精算する処理を行ってみよう。この場合、たとえば、図20①に示す「SELECT #1 DF1-1」なる選択コマンドを与え、チャンネル#1を更新すればよい。図20に示すように、記録部(3, 1)の識別情報が、DF 1-2からDF 1-1へと更新され、開錠情報は未開錠の状態となる。そこで、図21①に示す「VERIFY #1 K6 ????」なる照合コマンドおよび図21②に示す「VERIFY #1 K7 ????」なる照合コマンドを与えることにより、ファイル管理領域DF 1-1のキーK6、K7を開錠し、図21③に示す「WRITE #1 D111 REC8 (DATA)」なる書込コマンドを与えれば、データファイルD111の第8レコードに、医療費未精算額を示す(DATA)が書き込まれることになる。

【0061】続いて、外国為替処理を行うために、ファイル管理領域DF 1-2を選択する必要が生じたので、図22①に示す「SELECT #3 DF1-2」なる選択コマンドを与え、チャンネル#3を更新したとする。すると、図22に示すように、記録部(1, 3)の識別情報はMFのままであるが、記録部(2, 3)の識別情報はDF 1に更新され、記録部(3, 3)の識別情報はDF 1-2に更新される。こうして更新された記録

部の開錠情報は、原則として未開錠の状態となるが、上述した同一性維持を図るため、同じ識別情報をもった記録部が他のチャンネルにある場合には、開錠情報の複写処理を行う。図22の例では、DF 1なる同じ識別情報をもった記録部(2, 2)もしくは(2, 1)の開錠情報が、記録部(2, 3)へと複写されることになる。

【0062】<3-9:キーの照合その2>続いて、図23①に示すような「VERIFY #2 K8 ????」なる照合コマンドにより、ファイル管理領域DF 1についてのキーK8を照合する処理を行ったとする。キーK8が照合一致すれば、記録部(2, 2)の開錠情報は、「00101000」の状態から、「00101001」の状態へと更新され、図23②に示すような「WRITE #2 D11 REC7 (DATA)」なる書込コマンドを与えることにより、データファイルD11の第7レコードに(DATA)が書き込まれることになる。ところで、上述した同一性維持を図るためには、このような開錠情報の更新があった場合にも複写処理を行う必要がある。すなわち、図23に示すように、記録部(2, 2)の開錠情報が更新された場合には、同じDF 1なる識別情報をもった記録部(2, 1)および(2, 3)へ、更新された記録部(2, 2)の開錠情報を複写する処理が行われる。

【0063】このように、複写処理は、選択コマンドによりチャンネルが更新された場合だけでなく、照合コマンドにより開錠情報が更新された場合にも行う必要がある。要するに、特定の記録部の開錠情報が更新された場合には、同一の識別情報をもった記録部についても、同様の更新が行われるように複写処理を実行すればよい。

【0064】§4. CPU12の行う処理

上述した§3では、本発明に係るICカードの利用形態を、チャンネル設定領域の記録内容の変遷を追いつつ、具体例に即して説明した。このような利用形態を実現させるためには、結局、CPU12は各コマンドに対して次のような処理を行えばよいことがわかる。

【0065】<4-1:選択コマンド>特定のチャンネルを指定して特定のファイル管理領域を選択するコマンド(たとえば、図22①「SELECT #3 DF1-2」)が与えられたときには、選択されたファイル管理領域およびこれより上位階層のファイル管理領域の識別情報を、指定されたチャンネル設定領域内のそれぞれの階層に対応した記録部に書き込んで記録済状態とし、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態とする書込処理を行う(たとえば、図22参照)。そして、この書込処理によって、識別情報が更新されなかった記録部(図22の記録部(1, 3))については開錠情報をそのまま維持し、識別情報が更新された記録部については、この更新された識別情報と同一の識別情報(図22のDF 1)が記録されている他の記録部(図22の記録部(2, 2))が存在する場合に

は、この他の記録部に記録されている開錠情報をそのまま複写し、そのような他の記録部が存在しない場合には、未開錠を示す開錠情報を書き込む処理を行う（図22の記録部（3，3））。

【0066】<4-2：照合コマンド>特定のチャネルを指定して所定のキー照合を行うコマンド（たとえば、図23①「VERIFY #2 K8 ????」）が与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部（たとえば、図23の記録部（2，2））に記録されている開錠情報をキー照合の結果に基づいて更新する更新処理を行い、この最下層の記録部に記録されている識別情報と同一の識別情報（DF1）が記録されている別な記録部（たとえば、図23の記録部（2，1），（2，3））が存在する場合には、更新処理によって更新された開錠情報を、この別な記録部にそのまま複写する処理を行う。

【0067】<4-3：アクセスコマンド>特定のチャネルを指定して所定の対象ファイルをアクセスするコマンド（たとえば、図11③「READ #1 D11 REC8」）が与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部（たとえば、図11の記録部（2，1））に記録されている識別情報で特定されるファイル管理領域（DF1）内にアクセス対象ファイル（D11）が所属し、かつ、この最下層の記録部に記録されている開錠情報（「00101000」）が、アクセス対象ファイルのアクセス条件（たとえば、図5のコマンドグループ1の条件）を満足する場合に、アクセス対象ファイルに対するアクセスを可能とする。

【0068】§5. その他の実施例

以上、本発明を図示する実施例に基いて説明したが、本発明はこれらの実施例に限定されるものではなく、この他にも種々の態様で実施可能である。たとえば、上述の実施例では、図5に示すアクセス条件テーブルの参照ビットRを「1」にしておくことにより、上位階層の開錠情報を参照できることを説明した。この参照ビットRは、上述の実施例では、個々のファイルごとにそれぞれ設定していたが、個々のファイル管理領域ごとに1つの参照ビットRを設定してもよい。この場合、複数階層にわたって参照が行われることもありうる。たとえば、図3において、ファイル管理領域DF1-1について「参照する」の設定を行い、更に、ファイル管理領域DF1についても「参照する」の設定を行っておけば、たとえば、階層3のデータファイルD111に対するアクセスを行う場合には、ファイル管理領域DF1-1、DF1、MFの3つの開錠情報の各ビットごとの論理和をとった融合開錠情報に基づいて、アクセス条件の判断が行われることになる。

【0069】また、上述の実施例では、参照ビットRのビット状態に応じて、上位階層の開錠情報を「参照す

る」か「参照しない」かの設定を行っていたが、特定の階層については、常に「参照する」旨の設定を行うことも可能である。たとえば、最上位階層のファイル管理領域MFは、このICカードの記録領域全体を統括管理する領域であり、ICカード10をリーダライタ装置20に接続した後、まず第1の照合操作として、カード所有者キーなど基本的なキー照合操作が、このファイル管理領域MFについて行われるのが一般的である。そこで、実用上は、第2階層以下の各ファイル管理領域については、最上位階層のファイル管理領域MFの開錠情報を常に参照する旨の設定を行っておくと便利である。このような設定は、わざわざ参照ビットRを用いて行う必要はなく、ROM13内のプログラムに、常にファイル管理領域MFの開錠情報を参照するようなルーチンを組み込んでおけばよい。

【0070】なお、上述の実施例では、説明の便宜上、図7に示すような3×3の配列をもった記録部をRAM14内に定義する例を述べたが、実際には、最上位階層は必ずファイル管理領域MFが占めることになるので、最上位階層については、複数のチャネルを代表する単一の記録部のみを用意しておけば足りる。すなわち、図24に示すように、階層1としては、ファイル管理領域MF専用の記録部を1つだけ設けておけばよく、この記録部には、開錠情報を記録する領域だけを設けておけば足りる。このような構成にすれば、ファイル管理領域MF内の開錠情報については、チャネル間での複写処理も不要になる。

【0071】

【発明の効果】以上のとおり本発明によれば、携帯可能情報記録媒体において、用途ごとに別々のセキュリティ設定がなされ階層構造をもったファイルに対して、十分なセキュリティを確保しつつ使い勝手の良いアクセスが可能になる。

【図面の簡単な説明】

【図1】一般的なICカード10に、外部装置としてのリーダライタ装置20を接続し、アクセスを行っている状態を示すブロック図である。

【図2】階層構造をもった具体的なファイル管理領域を、EEPROM15内に定義した状態を示す概念図である。

【図3】図2に示すファイル管理領域および各ファイルの階層構造を示すツリー図である。四角で囲ったブロックはいずれもファイル管理領域を示し、楕円で囲ったブロックは個々のデータファイル（頭に記号Dのついたファイル）およびキーファイル（頭に記号Kのついたファイル）を示す。

【図4】各ファイル管理領域に、それぞれ大まかな用途を定義した一例を示すブロック図である。

【図5】EEPROM15内において、各ファイルについてのアクセス条件の設定例を示すアクセス条件テー

ルである。

【図6】RAM 14内に確保されるキーK1～K8の開錠状態を示す8ビットの領域を示す図である。

【図7】本発明において用いられるチャンネル設定領域の一例を示す図である。

【図8】図7に示すチャンネル設定領域の初期状態の記録内容を示す図である。

【図9】図8に示す初期状態において、チャンネル#1を用いてファイル管理領域DF1を選択するコマンドを実行した状態を示す図である。

【図10】図8に示す初期状態において、チャンネル#1を用いてファイル管理領域DF1-2を選択するコマンドを実行した状態を示す図である。

【図11】図9に示す状態において、ファイル管理領域DF1に対するキー照合コマンドを実行した状態を示す図である。

【図12】図11に示す状態において、チャンネル#1を用いてファイル管理領域DF1-2を選択するコマンドを実行した状態を示す図である。

【図13】図12に示す状態において、ファイル管理領域DF1-2に対するキー照合コマンドを実行した状態を示す図である。

【図14】上位階層の開錠状態を参照する処理を説明する図である。

【図15】図14に示す状態において、チャンネル#1を用いてファイル管理領域DF1を再選択するコマンドを実行した状態を示す図である。

【図16】図14に示す状態において、チャンネル#2を用いてファイル管理領域DF1を再選択するコマンドを実行した状態を示す図である。

【図17】図16に示す状態において、チャンネル#1を用いてファイル管理領域DF2-2を選択するコマンドを実行した状態を示す図である。

【図18】図16に示す状態において、チャンネル#3を*

*用いてファイル管理領域DF2-2を選択するコマンドを実行した状態を示す図である。

【図19】図18に示す状態において、ファイル管理領域DF2-2に対するキー照合コマンドを実行した状態を示す図である。

【図20】図19に示す状態において、チャンネル#1を用いてファイル管理領域DF1-1を選択するコマンドを実行した状態を示す図である。

【図21】図20に示す状態において、ファイル管理領域DF1-1に対するキー照合コマンドを実行した状態を示す図である。

【図22】図21に示す状態において、チャンネル#3を用いてファイル管理領域DF1-2を選択するコマンドを実行した状態を示す図である。

【図23】図22に示す状態において、ファイル管理領域DF1に対するキー照合コマンドを実行した状態を示す図である。

【図24】最上位階層について、複数のチャンネルを代表する単一の記録部のみを用意したチャンネル設定領域の一例を示す図である。

【符号の説明】

10…ICカード

11…I/Oインタフェース

12…CPU

13…ROM

14…RAM

15…EEPROM

D…データファイル

DF…ファイル管理領域

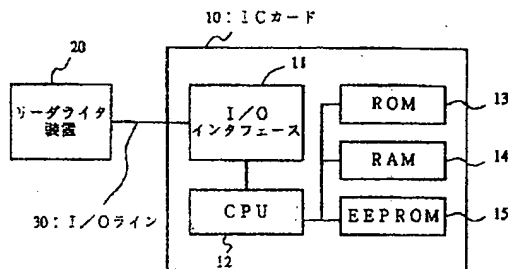
K…キーファイル

K1～K8…キー

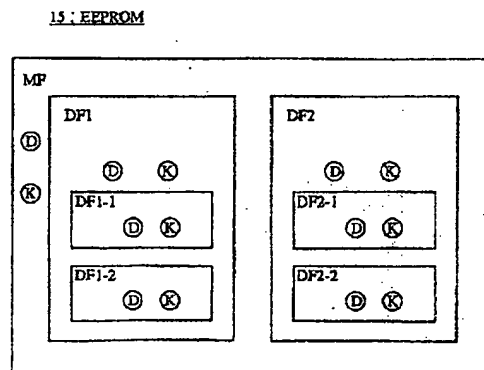
MF…最上位階層のファイル管理領域

R…参照ビット

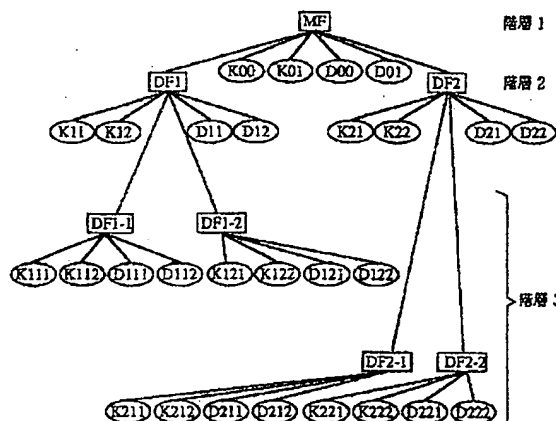
【図1】



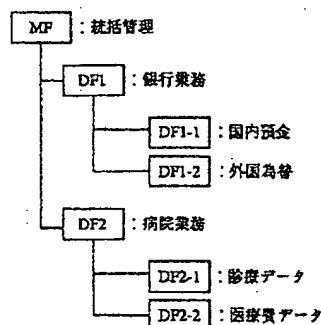
【図2】



【図3】



【図4】



【図5】

【図6】

1つのファイルについてのアクセス条件 (EEPROM15)

開錠情報 (RAM14)

R	K1	K2	K3	K4	K5	K6	K7	K8	
1	0	0	1	0	1	0	0	0	コマンドグループ1
0	1	0	0	0	1	0	0	1	コマンドグループ2
0	1	1	0	0	0	1	0	0	コマンドグループ3

(0: 開錠不要, 1: 開錠必要)

↑ 上位階層の開錠情報の参照の有無
(0: 参照せず, 1: 参照する)

(a)

K1	K2	K3	K4	K5	K6	K7	K8
0	0	0	0	0	0	0	0

(0: 未開錠, 1: 開錠)

(b)

K1	K2	K3	K4	K5	K6	K7	K8
0	0	1	0	0	0	0	0

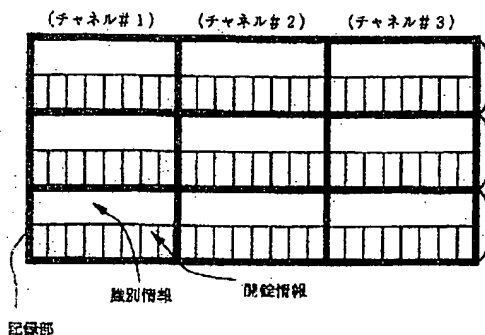
(c)

K1	K2	K3	K4	K5	K6	K7	K8
0	0	1	0	1	0	0	0

【図7】

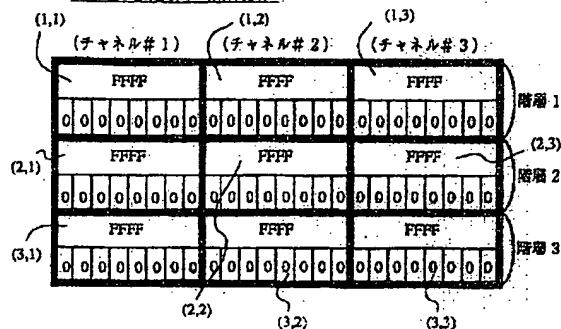
【図8】

チャンネル設定領域 (RAM14)

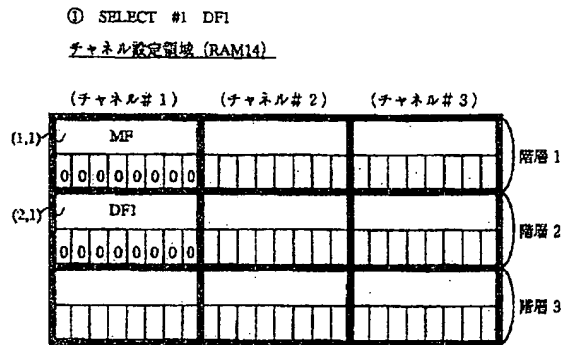


○初期状態

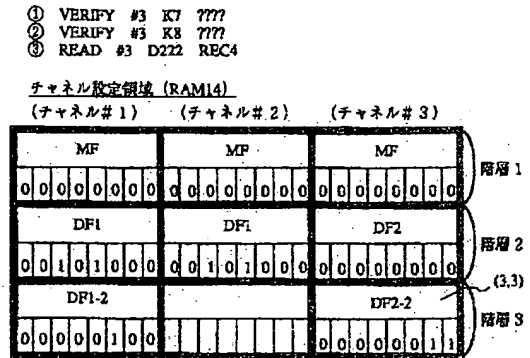
チャンネル設定領域 (RAM14)



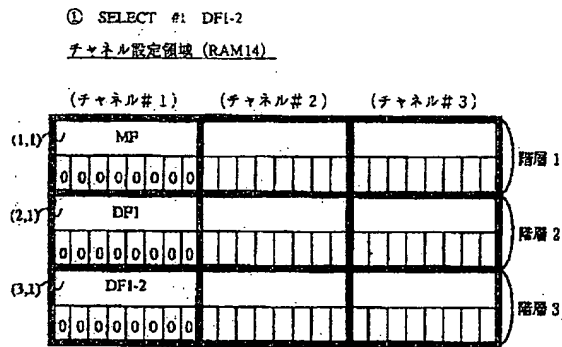
【図9】



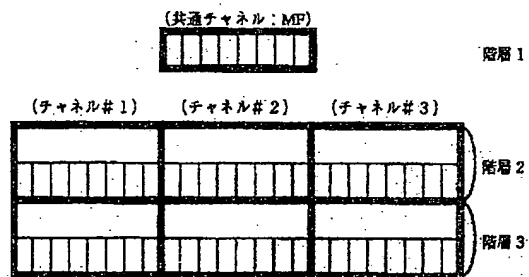
【図19】



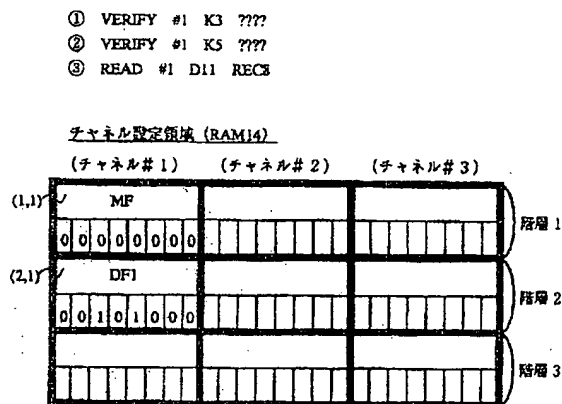
【図10】



【図24】



【図11】



【図12】

① SELECT #1 DF1-2

チャンネル設定領域 (RAM14)

	(チャンネル#1)	(チャンネル#2)	(チャンネル#3)
(1,1) MF	00000000		
(2,1) DF1	00101000		
(3,1) DF1-2	00000000		

階層 1
階層 2
階層 3

【図17】

① SELECT #1 DF2-2

チャンネル設定領域 (RAM14)

	(チャンネル#1)	(チャンネル#2)	(チャンネル#3)
(1,1) MF	00000000	00000000	
(2,1) DF2	00000000	00101000	
(3,1) DF2-2	00000000		

階層 1
階層 2
階層 3

【図13】

- ① VERIFY #1 K3 ????
- ② VERIFY #1 K5 ????
- ③ VERIFY #1 K6 ????
- ④ READ #1 D121 RECS

チャンネル設定領域 (RAM14)

	(チャンネル#1)	(チャンネル#2)	(チャンネル#3)
(1,1) MF	00000000		
(2,1) DF1	00101000		
(3,1) DF1-2	00101100		

階層 1
階層 2
階層 3

【図20】

① SELECT #1 DF1-1

チャンネル設定領域 (RAM14)

	(チャンネル#1)	(チャンネル#2)	(チャンネル#3)
(1,1) MF	00000000	00000000	00000000
(2,1) DF1	00101000	00101000	00000000
(3,1) DF1-1	00000000		00000011

階層 1
階層 2
階層 3

【図14】

- ① VERIFY #1 K6 ????
- ② READ #1 D121 RECS

チャンネル設定領域 (RAM14)

	(チャンネル#1)	(チャンネル#2)	(チャンネル#3)
(1,1) MF	00000000		
(2,1) DF1	00101000		
(3,1) DF1-2	00000000		

階層 1
階層 2
階層 3

(3,1)

【図21】

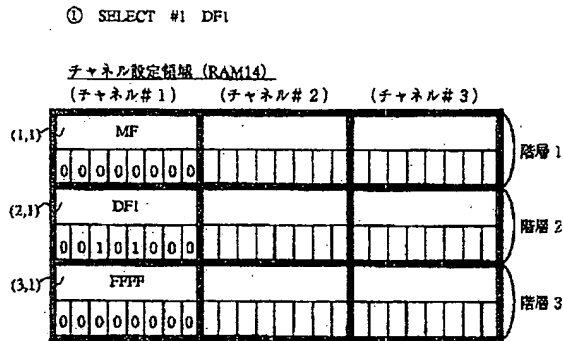
- ① VERIFY #1 K6 ????
- ② VERIFY #1 K7 ????
- ③ WRITE #1 D111 RECS (DATA)

チャンネル設定領域 (RAM14)

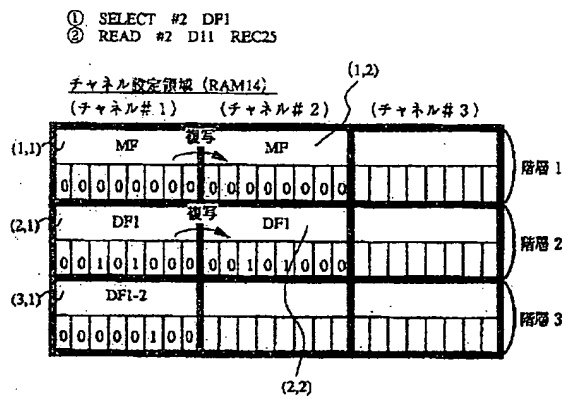
	(チャンネル#1)	(チャンネル#2)	(チャンネル#3)
(1,1) MF	00000000	00000000	00000000
(2,1) DF1	00101000	00101000	00000000
(3,1) DF1-1	00000011		00000011

階層 1
階層 2
階層 3

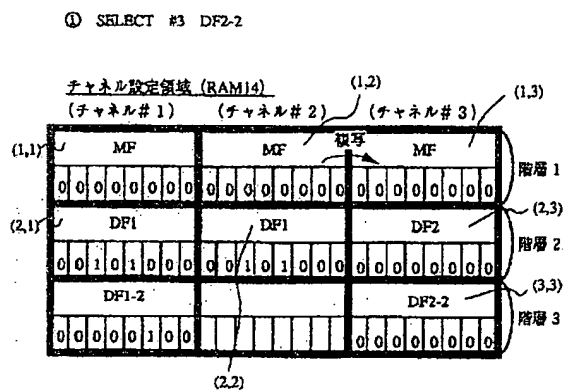
【図15】



【図16】

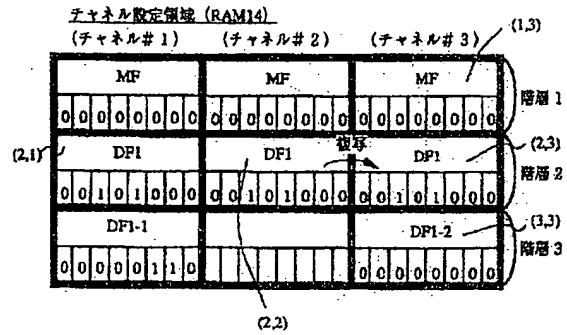


【図18】



【図22】

① SELECT #3 DF1-2



【図23】

① VERIFY #2 K8 777?
② WRITE #2 D11 REC7 (DATA)